

As previously discussed, England discloses a digital rights management operating system involving a number of certificates including a manufacturer certificate 166, CPU certificate 202, and rights manager certificate 210. England does not disclose or suggest that any of these certificates are generated in the manner required by Applicant's claim 1. Specifically, England fails to disclose or suggest a public key of a software signature site and a secret key of a control entity of a trust center. The Office Action, however, continues to rely on the disclosure of England to support the obviousness rejection.

The Office Action cites column 7, line 63 – column 8, line 14 of England for the disclosure of a secret or private key of a software signature site for signing software. The Office Action states that this section discloses a “software developer or manufacturer digitally signs software before use; private (secret) key of manufacturer's CPU (control entity).” First, this section does not mention a “manufacturer's CPU.” Second, this section does not mention that software is signed. Rather, this section is directed to producing certificate 166 testifying that a CPU was produced according to a known specification and does not disclose or suggest a software signature site. Even if it were assumed that the manufacturer is a software developer, there is no disclosure or suggestion that the manufacturer's public key is “of the software signature site” as required by claim 1.

The Office Action further cites column 8, line 66 – column 9, line 3 of England for the alleged disclosure of a trust center or trusted third party for certificate signing. As previously argued, this cited portion of England discloses

that “operating system-level components [are] digitally signed by their developers or a trusted third party”. Notably absent from this or any other portion of England is any disclosure or suggestion of a secret key of a control entity of a trust center. Further, England does not disclose or suggest any relationship between the “third party” and manufacturer certificate 166. Accordingly, England does not disclose or suggest generating a software signature certificate in the manner recited in Applicant’s claim 1.

The Office Action acknowledges that England does not disclose generating a certificate using a public key and a secret key, and instead relies upon Davis for such a disclosure.

Davis discloses a method for implementing a key pair and digital certificate into a semiconductor device.¹ Although Davis discloses a key pair, Davis does not disclose or suggest that the key pair relates a public key of a software signature site and a secret key of a control entity of a trust center. In contrast to the method recited in Applicant’s claim 1, Davis discloses a random number generator to generate key pairs.²

The Office Action cites column 5, lines 43-59 of Davis for the disclosure of generating a signature certificate using the public key of the signature site and a secret key of a control entity, according to a public key method. This section discloses signing a public key of a hardware device with a manufacturer’s private key for a hardware device. Like England, Davis does not disclose or suggest that the public key is associated with a software signature site. Moreover, Davis fails

¹ Abstract.

² Column 5, lines 31-33.

to disclose or suggest that the manufacturer key is associated with a control entity of a trust center. Accordingly, Davis does not remedy the deficiencies of England.

As previously argued, Wong does not disclose generating a software signature certificate and thus, does not remedy the deficiencies of Applicant's claim 1. Applicant respectfully submits that the combination of England, Davis and Wong does not disclose or suggest generating a software signature certificate as required by claim 1.

Claims 3-6 and 8-18 are patentably distinguishable over the combination of England, Davis and Wong at least by virtue of dependency from claim 1.

Independent claim 7 recites a method involving a software signature certificate, and is patentably distinguishable over the combination of England, Davis and Wong for similar reasons to those discussed above with respect to claim 1.

Regarding Applicant's independent claim 19, the Office Action cites column 11, lines 54-59 of England for checking if the software signature certificate has been changed or manipulated. A disclosure of checking a signature, based solely on signature validity, does not, however, disclose or suggest checking a software signature certificate for change or manipulation as recited in claim 19. Neither Davis nor Wong remedy the deficiencies of England with respect to claim 19. Claim 20 is patentably distinguishable over the combination of England, Davis and Wong at least by virtue of its dependency from claim 19.

Claim 20 is rejected under 35 U.S.C. § 112, second paragraph for indefiniteness. The Office Action alleges that there is no disclosure of a third public key and a third signature within the specification or the original claims. Applicant respectfully submits that this is not a proper rejection under U.S.C. § 112, second paragraph. Specifically, the claim language “a third public key” and “a third signature” are each definite. These terms particularly point out and distinctly claim the subject matter of the claims. As previously argued, if a description or the enabling disclosure of a specification is not commensurate in scope with the subject matter encompassed by a claim, that fact alone does not render the claim imprecise or indefinite or otherwise not in compliance with 35 U.S.C. § 112, second paragraph.³

Applicant respectfully submits that not only is claim 20 definite, but also it is fully supported by the original disclosure of the application. Fig. 1 of Applicant's disclosure discloses a trust center signature certificate 116 comprising a key 101 and signature 117 (e.g., first key and first signature), clearing code site software signature certificate 118 comprising a key 106 and signature 119 (e.g., second key and second signature), and software signature certificate 120 comprising a key 108 and signature 121 (e.g., third key and third signature). Thus, the original application provides support for the claimed third public key and third signature. Accordingly, withdrawal of this rejection is respectfully requested.


³ MPEP 2174.

If there are any questions regarding this response or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 080437.53236US).

Respectfully submitted,

October 7, 2009



Stephen W. Palan
Registration No. 43,420
John P. Teresinski
Registration No. 56,621

CROWELL & MORING, LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
SWP:JPT/cee